UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/764,504	01/27/2004	Kouhei Nadehara	Q79582	9262

23373 7590 09/18/2008

SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037

EXAMINER	
BESROUR, SAOUSSEN	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
09/18/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/764,504	NADEHARA, KOUHEI	
	Examiner	Art Unit	
	SAOUSSEN BESROUR	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/29/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed 1/26/2004.

2. Claims 1-14 were received for consideration.

3. No preliminary amendments for the claims were filed. Currently claims 1-

1-14 are under consideration.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. **Claims 1-14** are rejected under 35 U.S.C. 102(e) as being anticipated by Van Buer (20030198345).

As per **claim 1, 3, 6 and 8**, Van Buer discloses: a selector unit selecting an element of a state in response to row and column indices (0007);
a S-box for obtaining a substitution value with said selected element used as an index (0063); a coefficient table providing first to fourth coefficients in response to said row index (0055, 0063); first to fourth Galois field multiplexers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with first

to fourth coefficients, respectively (0054, 0055, 0058, 0063-0064); and

an accumulator which accumulates the first to fourth products to develop first to fourth elements of a designated column of a resultant state (0067-0070).

As per **claim 11, 12 and 14**, Van Buer discloses a first selector unit selecting an element of a state in response to row and column indices (0007);

an inverse affine transformation circuit applying an inverse affine transformation on said selected element (0059-0063);

a second selector unit selecting one out of two data bytes consisting of said selected element received from said first selector, and a result of said inverse affine transformation received said inverse affine transformation circuit, wherein said selected element is selected for encryption, while said result of said inverse affine transformation is selected for decryption (Fig. 25);

an inverse determining unit obtaining a multiplicative inverse of said selected data byte received from said second selector (Fig. 25);

an affine transformation circuit applying 20 an affine transformation on said obtained multiplicative inverse (0063);

a third selector unit selecting one of two data bytes consisting of said multiplicative inverse received from said inverse determining unit, and a result of said affine transformation received from affine transformation circuit, wherein said result of said affine transformation is selected for decryption, while said multiplicative inverse is

selected for encryption (0066-0067);

a coefficient table providing first to fourth coefficients in response to said row index;

first to fourth Galois field multiplexers respectively computing first to fourth products, which are obtained by multiplication of said

substitution value with first to fourth coefficients, respectively (0055, 0063); and

an accumulator which accumulates the first to fourth products to develop first to fourth elements of a designated column of a resultant state (0054, 0055, 0058, 0063-0064).

As per **claim 2, 5, 7, and 10**, Van Buer discloses: wherein said first to fourth coefficients are respectively set to {02}, (01}, {01}, and {03} in response to said row index selecting a first row of said state, to {03}, {02}, (01}, and (01} in response to said row index selecting a second row of said state, to (01}, (03}, (02}, and (01} in response to said row index selecting a third row of said state, and to {01}, {01), {03}, and {02) in response to said row index selecting a fourth row of said state (0070-0075).

As per **claims 4, 9 and 13**, Van Buer discloses: a processing unit adapted to implement XORing, wherein said AES encryption processor is further adapted to an XOR instruction, and wherein said processing unit implements XORing of values contained in two selected registers of said register file (0060).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SAOUSSEN BESROUR whose telephone number is (571)272-6547. The examiner can normally be reached on M-F 8:30am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. B./
Examiner, Art Unit 2131
September 16, 2008

/Syed Zia/
Primary Examiner, Art Unit 2131